

# Towards Automated Modelling of Large-scale Cybersecurity Transformations: Potential Model and Methodology

Artur Rot<sup>a</sup> and Bartosz Blaićke<sup>b</sup>

*Department of Information Systems, Wrocław University of Economics, Wrocław, Poland*

**Keywords:** Security, Cybersecurity, Transformation, Investment, Budget, Risk-based Approach.

**Abstract:** The purpose of this paper is to propose a proprietary methodology and model to generate a “cybersecurity transformation workplan” for large organizations that can improve their cybersecurity posture. The key input is based on risk-based assessment or maturity-based questionnaires depending on existing governance processes and available information. The original scoring can be then used to prioritize a portfolio of all possible initiatives by selecting the ones that are missing from typical foundation elements or would have high potential impact in relation to required investment and effort. Additional constraints such as budget limitation and FTE availability, logical sequencing and time requirements could be added to ensure effective use of company resources and actionability of the recommendations. The Gantt-like output would ease the burden on the security teams by providing an individualized set of activities to be implemented to improve risk posture.

## 1 INTRODUCTION


Cybersecurity is a field that has been gaining significant attention among IT professionals and the general public. Part of the reason is due to rising prominence of cyber-attacks and their impact so that they are now considered one of the top 5 global risks on par with extreme weather events and natural disasters (WEF, 2019). However, even considered on their own, cyberattacks are becoming increasingly dangerous. They are growing in quantity at a 34% per year (US-GAO, 2016), sophistication such as recent Triton attack that could override itself to cover its tracks (Venkatachary, Prasad and Samikannu, 2018) and reach as single modern ransomware (e.g. NotPetya) is able affect computers in more than 100 countries worldwide (Jasper, 2017). Unfortunately, the defense perimeter is enormous, and attackers only need a single-entry vector to be successful so not only many attacks go unnoticed with average time to detection being multiple months, but many more are believed to go completely unnoticed (Verizon, 2017).


There is also significant innovation element in cybersecurity with more than USD 20bn of merger and acquisition spending in the space and additional

USD 5bn being invested by private equity companies into disruptive cybersecurity start-ups in 178 deals during 2017 alone (McAlpine et al, 2018). Regrettably, some of that innovation causes more confusion with companies having to setup and manage multiple provider ecosystems each operating separately and adding complexity that often is not leading to more security but opening another potential attack vector for attackers due to misconfigurations.

Internet of Things (IoT) adds another layer of complexity with the proliferation of over 30bn connected devices predicted to be online by 2023 (Ericsson, 2017) that can often be easily discoverable via “Google-like” search engines such as SHODAN and accessed by anyone using default passwords. Such services expose hundreds of thousands IoT devices, many with unchangeable default passwords and no future firmware updates. (Rot and Blaićke, 2017).

Attacks have also already crossed the digital-physical barrier as long ago as 2010. We have seen that cyberattacks can cause physical consequences or even be used as military weapons that are highly targeted and potentially more effective than traditional warfare such as Stuxnet (Zetter, 2014).

<sup>a</sup>  <https://orcid.org/0000-0002-7281-8253>

<sup>b</sup>  <https://orcid.org/0000-0002-5083-0059>

Malicious actors are now targeting utilities and energy sector companies, as much as 68% of all such companies were hit by a cyber-attack in 2016 (Ponemon, 2017).

All the complexity for businesses is further amplified by shortage of adequate talent, that doesn't even come close to match current demand and will not do so for the foreseeable future (Libicki, Senty and Pollak, 2014). That often results in inadequate attention to the issue despite significant threat that cyber adversaries pose to our increasingly digital society.

Therefore, the purpose of this paper is to propose proprietary methodology that could take away some of the complexity by automating part of the planning and give organizations a "fighting chance". Focusing their activities on more initiatives that would increase their odds against potential attacks would be the first step in that direction and we are hoping this paper could provide that.

## 2 STATE OF THE ART APPROACH TO CYBERSECURITY TRANSFORMATIONS

Traditionally cybersecurity transformation planning has been done either by senior cybersecurity function employees (i.e. CISO or N-1) that often have many competing and immediate responsibilities or crises to handle preventing them from devoting all the necessary time and attention to such long-term activities. Therefore, more often due to the increased scrutiny from the board of directors (Rothrock, Kaplan and Van der Oord, 2017) 3<sup>rd</sup> party specialists or management consulting companies are brought in for several weeks or months to deliver such custom-tailored plans.

The problem is also being discussed within the academia with various approaches such as cybersecurity investment supply chain game theory model (Nagurney, Nagurney and Shukla, 2015), focusing on how to optimally invest in cybersecurity controls when organizations are underinvesting (Panaousis et al, 2014) or how to use economic incentives for cybersecurity (Vishik, Sheldon and Ott, 2013).

The use of 3<sup>rd</sup> party vendor typically requires significant investment that is not always available for organizations. On the other hand, none of the academic approaches have been described and documented yet in such a way that would allow for

easy implementation or as a matter of fact tested in a real-life scenario. Therefore, we can build on all these experiences to enhance the proposed model before testing that as a real-life scenario.

## 3 PLANNING CYBERSECURITY TRANSFORMATIONS

In response to the increased complexity and threat, companies are significantly increasing spending for cybersecurity. In 2019 analysts estimate that excess of USD 124bn will be spend on information security which is a 12.4% increase from last year (Gartner, 2018). However, that increasing spending is not necessarily correlated with better security for the companies as there is a vast spectrum of companies spending above average on security as proportion of IT spending achieving similar or even lower security ratings than their peers. In addition, traditional cybersecurity focus is on controls and processes. However, there are further layers that need to be addressed to fully cover the area including organization aspects (e.g. organization structure) or governance (e.g. roles and responsibilities). Historically, spending is focused on technology such as firewalls, intrusion prevention systems or identity and access management solutions but not necessarily with business outcomes in mind or understanding the impact these solutions would have on the remaining part of the organization (Choi et al, 2017).

Cybersecurity transformations in such an environment needs to consider what is already established and existing within an organization. Depending on that, it needs to find a balance between technical and business-related activities that should be implemented. In addition, a mix of long-term efforts and quick wins should be established to protect against current treats quickly but also start laying down the foundations for protection mechanisms of tomorrow.

### 3.1 Establishing the Baseline

The key input needed before considering what needs to be recommended as part of a cybersecurity function transformation is a complete understanding of the current state. That could be gained following two different approaches, depending on existing elements at a given organization:

- Risk-based approach that is rooted in a more detailed assessment of threats, vulnerabilities and controls that results in risk exposures with various

likelihoods. It requires more effort and is typically found only in more advanced organizations.

- Maturity-based approach has been historically the preferred method due to easier implementation. It has certain limitations as it is often self-reported and carries a potential danger of targeting a certain maturity level without an established link to actual improvement of the security posture.

### 3.1.1 Risk-based Approach

Risk-based approach is a methodology that encourages organizations to clearly identify, list and assess risks that they are exposed to. That understanding is used to focus effort and resources on addressing highest risks first and deploying adequate protection to other risks. To follow a risk-based approach the company needs to create and maintain a list of potential threats, up-to-date status of vulnerabilities across the environment and controls that are in place and planned to mitigate known vulnerabilities that jointly could also be thought of as likelihood of the risk. All that will inform the well-established equation (1).

$$\text{Risk} = \text{Threats} \times \text{Vulnerabilities} \times \text{Impacts} \quad (1)$$

That level of understanding is already very helpful for the security function on its own. In addition, as it provides detailed understanding of controls and vulnerabilities it allows to effectively target the controls and initiatives with the potential to maximize vulnerability reduction.

### 3.1.2 Maturity-based Approach

Alternatively, a simpler and still very popular method is to follow a maturity-based approach. Its goal is to showcase how advanced any organization is by assigning a cybersecurity preparedness score or a rank to each area, often on a 5-point scale from 0 being non-existent, 1 inadequate, to 4 considered advanced or state-of-the-art. Such maturity score is mostly based on self-reported questionnaires covering multiple elements of a cybersecurity organization from governance, through existing technical controls to personnel awareness level (often ~100 questions). The score allows to prioritize areas requiring immediate improvement.

## 4 DEVELOPING A PORTFOLIO OF INITIATIVES

Following initial phase of assessing the current state of the organization, next step would include comparing

the individual risks or maturity scores with a proprietary model of all potential activities that can be recommended. That will inform which actions are necessary as well as how they should be prioritized in a most efficient way given existing constraints.

### 4.1 Segmentation Framework Options

To cover the entire realm of potential initiatives we need to establish a framework that will be comprehensive but also intuitive enough for the cybersecurity function to include it into their processes. The most obvious choice for such frameworks are industry standards such as ISO 27001 and 27002 or NIST Cybersecurity Framework (CSF) but there are also proprietary approaches such as Resilience Levers used by McKinsey & Company that should be compared. A brief overview of primary areas highlighted by each of the above mentioned frameworks shows different segmentation and level of detail available as shown in Table 1.

Table 1: Comparison of key areas for each framework.

ISO 27002	NIST CSF	Resiliency Levers
Information security policies	Identify	Information assets and related risks
HR security	Protect	Frontline personnel
Organization of information security	Detect	Resilience in enterprise processes
Asset management	Respond	Incident response
Access control	Recover	Security integration into technology
Cryptography	n/a	Differentiated protection for assets
Physical and environmental security	n/a	Deploy active defenses
Operations security	n/a	n/a
Communications security	n/a	n/a
System acquisition, development and maintenance	n/a	n/a
Supplier relationships	n/a	n/a
Incident management	n/a	n/a
Business continuity management	n/a	n/a
Compliance	n/a	n/a

Despite the differences, all the activities could also be mapped against all the frameworks simultaneously at deeper levels if needed, providing another layer of comparison.

## 4.2 Prioritization Approach

Having the framework selected, we would need to establish a large portfolio of initiatives that would cover multiple possible scenarios that a company might find itself in. Sample set of initiatives could include the following:

- Launch phishing campaigns with real-time feedback for users;
- Set common vision and mission for the cybersecurity function in line with business objectives;
- Introduce Network Access Control (NAC) solution(s).

The model would capture the following proprietary attributes for each of the activities in the baseline portfolio:

- Actionable description;
- Cybersecurity areas that an activity would impact based on selected taxonomy;
- Estimate of time needed to implement (adjustable based on company data such as revenue and FTEs – detailed in 5.1);
- Sequencing/prioritization within each taxonomy section (based on logical flow of implementation activities) and globally (based on overall impact and interdependencies);
- Two high level indicators whether this would be a “quick win” (less than a month) or a longer-term endeavor as well as if that would be a “basic, intermediate or advanced” type of control once implemented;
- Estimated impact on the initial self-assessment score (maturity or risk-based) if that activity would be completed;
- Flags for omitting an activity (already in place) or indicating current work in progress or manual prioritization modifier.

Combination of the input scoring and full portfolio prioritization would result in each activity being marked as relevant or not and prioritized accordingly to their risk reduction or maturity score improvement to form an individual output. That allows to accommodate for the fact that not every element needs to reach the highest possible risk reduction potential or maturity, nor would it be effective use of company resources in most cases.

## 5 GENERATING AND ADJUSTING THE OUTPUT PLAN

The final element once the input and initial prioritization are complete, is to adjust the output and recommendations in a way that would make it relevant and usable for an organization. One way to do it is to allow for certain constraints to be defined so that the desired plan is relatable and realistic. For example, if we were to propose an estimated effort to be 10 times larger than what the organization could typically handle than such recommendation is not going to be taken seriously. However, if we can distill which actions would be the best candidates within the budget constraints that would result in a solid foundation that could be used as a starting point by the security function. Secondly, the output presentation element is equally important since “a picture is worth a thousand words” and having a visual representation with easily accessible details is crucial.

### 5.1 Constraints Handling

Each company at any given moment in time is operating in a unique environment with different constraints following a different vision and plan. To be able to make the recommendations relatable, the activities need to be adjustable based on the following criteria:

- Company size based on revenue or Full Time Equivalent (FTE);
- Allocated cybersecurity budget;
- Size of the cybersecurity team;
- Number of potential concurrent efforts that could be handled simultaneously;
- Aspiration level to be achieved (e.g. reduction of risk by X% or maturity score improvement by Y points).

Modifying these criteria would allow to adjust the baseline output as close to the desired state as possible. However, while it is possible to make these modifications, it is not required as it might also be beneficial to understand the long tail of what needs to be done as the first iteration before proceeding to adjust the scope.

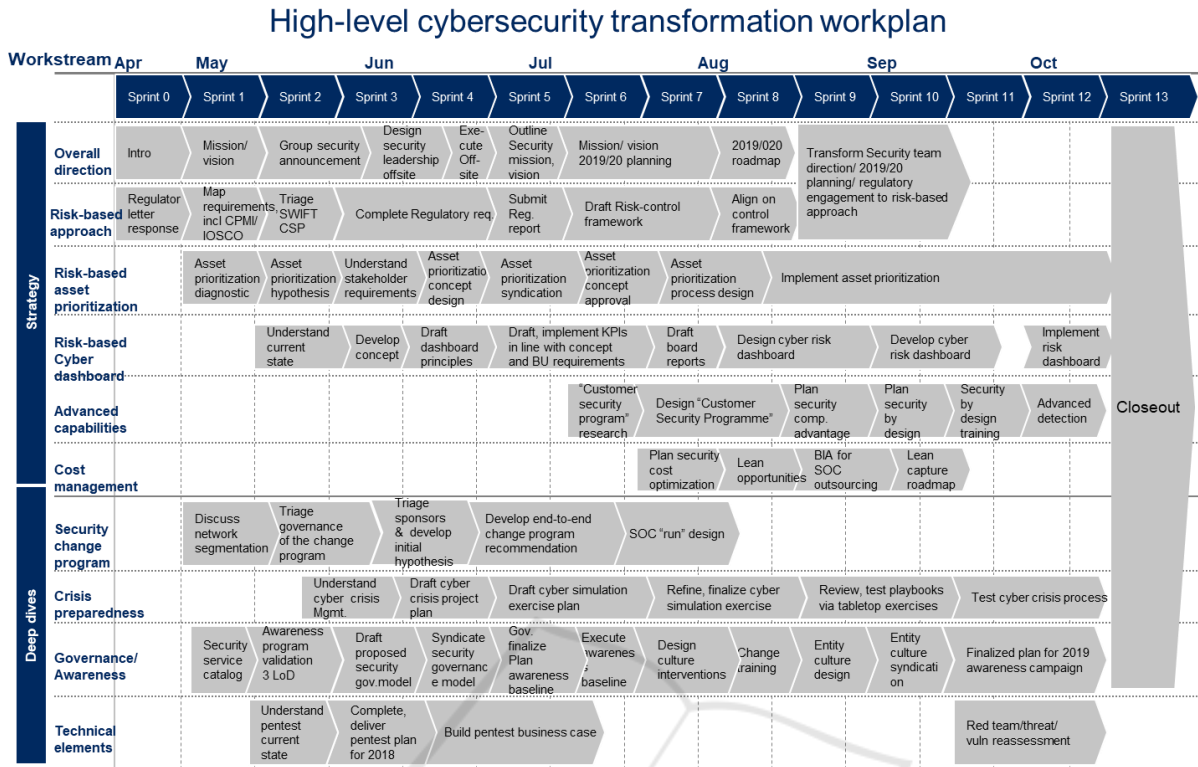


Figure 1: Potential visual representation of the output.

## 5.2 Output Generation

The output from the model would be a Gantt chart (see Figure 1 as an example based on previous manually prepared case study) offering an overview of all the recommended activities, put in a sequence with an estimate of man-hours needed to complete the entire plan. Such output would be modifiable using previously discussed constraints criteria that the organization would like to apply. Proposed automatization approach should be a ranking or points-based system with multiple parameters to initially address the sequencing aspect. In addition, it should be aided with algorithms for multi-project scheduling such as presented for IT development efforts (Chen et al, 2017). The added complexity is that it would need to operate under time dependent uncertainty because early in the planning exact initiatives durations are highly uncertain as proposed more generally in (Song et al, 2019). Potentially with large enough sample set a machine learning algorithm could be used to further automate the process and improve the output quality. However, early on following a simultaneous manual process to validate and adjust the automated output would be key to ensure high quality and allow for adjustments to the model.

Such proposed work plan could then be used directly as a high-level blueprint for an organization to start improving their cybersecurity function or further modified by the security team for their specific needs. Additional adjustments could be based on state of individual projects or activities that might overlap with what IT or other adjacent functions are performing for additional customization.

## 6 CONCLUSIONS

We began this paper with an overview of how cybersecurity is gaining importance but remains a complex challenge for most organizations. After examining current state, we concluded that such fundamental issue as holistic improvement of individual company cybersecurity posture is not easily solved with currently available methods. Some of which are too abstract and theoretical while others do not scale well and require additional expenditure that might place them out of reach for some organizations.

Thus, we hope that our early thinking on the proposed proprietary approach and methodology described in this position paper provides an

explanation of how automating the modelling of large-scale cybersecurity transformations can be done in an approachable way. We believe that is an important problem that we could solve or at the very least simplify for all the organizations that are looking to improve their cybersecurity posture in an efficient way.

Fully developing the described methodology and model would allow to shorten the time and effort needed to create such comprehensive transformation plans and, in some cases, might be enough to get the company on the right track immediately.

## REFERENCES

- Chen, R., Liang, C., Gu, D., Leung, J., 2017. *A multi-objective model for multi-project scheduling and multi-skilled staff assignment for IT product development considering competency evolution*, International Journal of Production Research, Issue 21, Volume 55, May 2017.
- Choi, J., Kaplan, J., Krishnamurthy, C., Lung, H., 2017. *Hit or myth? Understanding the true costs and impact of cybersecurity programs*. <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs>. Accessed Jan 2019.
- Ericsson, 2017. *Ericsson Mobility Report with Middle East and Africa Appendix, November 2017*. <https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-november-2017-middle-east-and-africa.pdf>. Stockholm, Sweden. Accessed Jan 2019.
- Gartner Inc., 2018. *Gartner Forecasts Worldwide Information Security Spending to Exceed \$124 Billion in 2019*, United States. <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>. Accessed Jan 2019.
- Jasper, S., 2017. *Russia and Ransomware: Stop the Act, Not the Actor*. The National Interest, November 20, 2017. USA.
- Libicki, M., Senty, D., Pollak, J., 2014. *Hackers Wanted: An examination of the cybersecurity labor market*, Rand National Security Research Division. Santa Monica, California, USA.
- McAlpine, E., Tedesco, M., Skirbe, K., Boukouris, D., Isagon, J., Keswani, J., 2018. *Cybersecurity Almanac*. [https://momentumcyber.com/docs/Yearly/2018\\_Cybersecurity\\_Almanac.pdf](https://momentumcyber.com/docs/Yearly/2018_Cybersecurity_Almanac.pdf). Accessed Jan 2019. Momentum Cyber, San Francisco, USA.
- Nagurney, A., Nagurney, L.S., Shukla, S., 2015. *A Supply Chain Game Theory Framework for Cybersecurity Investments Under Network Vulnerability*. Amherst, USA.
- Panaousis, E., Fielder, A., Malacaria, P., Hankin, C., Smeraldi, F., 2014. *Cybersecurity Games and Investments: A Decision Support Approach*. Queen Mary University of London, UK.
- Ponemon Institute, 2017. *The state of cybersecurity in the oil & gas industry*, United States. [http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press\\_release/additional/Cyber\\_readiness\\_in\\_Oil\\_Gas\\_Final\\_4.pdf](http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil_Gas_Final_4.pdf). Accessed Jan 2019.
- Rot, A., Blaike, B., 2017. *Internet of Things security. Selected threats and protection methods on the example of manufacturing systems*, Publishing House of Czestochowa Technical University, Czestochowa, Poland.
- Rothrock, R.A., Kaplan, J., Van der Oord, F., 2017. *The Board's Role in Managing Cybersecurity Risks*, MIT Sloan Management Review Magazine: Winter 2018 Issue. Cambridge, USA.
- Song, W., Kang, D., Zhang, J., Cao, Z., Xi, H., 2019. *A Sampling Approach for Proactive Project Scheduling under Generalized Time-dependent Workability Uncertainty*, Journal of Artificial Intelligence Research Volume 64, 2019.
- United States Government Accountability Office (US-GAO), 2016. *Information Security. Agencies Need to Improve Controls over Selected High-Impact Systems*. <https://www.gao.gov/assets/680/677293.pdf> Washington DC., USA. Accessed Jan 2019.
- Venkatachary, S.K., Prasad, J., Samikannu, R., 2018. *Cybersecurity and cyber terrorism - in energy sector – a review*. Journal of Cyber Security Technology Volume 2, 2018.
- Verizon, 2017. *Data Breach Investigations Report 10<sup>th</sup> Edition*, USA. <http://www.verizonenterprise.com/verizon-insights-lab/dbir/tool/>. Accessed Jan 2019.
- Vishik, C., Sheldon, F., Ott, D., 2013. *Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment*.
- World Economic Forum (WEF), 2019. *The Global Risks Report 2019, 14th Edition*. Geneva, Switzerland. [http://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2019.pdf](http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf). Accessed Jan 2019.
- Zetter, K., 2014. *Countdown to zero day. Stuxnet and the launch of the world's first digital weapon*, Random House. USA.